

---

# WESCO Net

---

**REPORT ON CONTROLS  
PLACED IN OPERATION AND  
TESTS OF OPERATING EFFECTIVENESS  
FOR WESCO Net**

*For the Period*

**January 1, 2010 through June 30, 2010**



South Bend, Indiana 46601  
<http://www.crowehorwath.com>

---

# WESCO Net

## REPORT ON CONTROLS PLACED IN OPERATION AND TESTS OF OPERATING EFFECTIVENESS

For the Period  
January 1, 2010 through June 30, 2010

### Table of Contents

<b>REPORT OF INDEPENDENT ACCOUNTANTS.....</b>	<b>1</b>
<b>DESCRIPTION OF CONTROLS PLACED IN OPERATION</b>	
Provided by WESCO Net	
<b>OVERVIEW OF OPERATIONS.....</b>	<b>3</b>
<b>GENERAL CONTROLS.....</b>	<b>7</b>
Organization and Administration.....	7
Physical Security .....	8
Managed Host Services (aka Facilities Management).....	9
Firewall Management Service.....	11
Complete Care Management.....	13
e-Business Policies and Procedures.....	15
<b>APPENDICES</b>	
Appendix A - Control Objectives, Policies, and Procedures.....	17
Appendix B - User Control Considerations.....	31
Appendix C - Organizational Chart.....	32



## REPORT OF INDEPENDENT ACCOUNTANTS

WESCO Net  
Grand Rapids, Michigan

We have examined the accompanying "Description of Controls Placed in Operation" related to the managed services of WESCO Net (WESCO Net). Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of WESCO Net's controls related to the managed services that may be relevant to a user organization's internal control as it relates to an audit of financial statements, (2) the controls included in the description were suitably designed to achieve the control objectives specified in the description, if those controls were complied with satisfactorily and user organizations applied the controls contemplated in the design of managed service controls and (3) such controls had been placed in operation as of June 30, 2010. The control objectives were specified by WESCO Net. Our examination was performed in accordance with standards established by the American Institute of Certified Public Accountants and included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

In our opinion, the accompanying description of the aforementioned application presents fairly, in all material respects, the relevant aspects of WESCO Net's controls related to the managed services that had been placed in operation as of June 30, 2010. Also, in our opinion, the controls, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily and user organizations applied the controls contemplated in the design of WESCO Net's controls related to the managed services.

In addition to the procedures we considered necessary to render our opinion as expressed in the previous paragraph, we applied tests to specific controls, listed in Appendix A, to obtain evidence about their effectiveness in meeting the control objectives, described in Appendix A, during the period from January 1, 2010 to June 30, 2010. The specific controls and the nature, timing, extent, and results of the tests are listed in Appendix A. This information has been provided to user organizations of the managed services at WESCO Net and to their auditors to be taken into consideration, along with information about the internal control at user organizations, when making assessments of control risk for user organizations. In our opinion, the controls that were tested, as described in Appendix A, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified in Appendix A were achieved during the period from January 1, 2010 to June 30, 2010. However, the scope of our engagement did not include tests to determine whether control objectives not listed in Appendix A were achieved; accordingly, we express no opinion on the achievement of control objectives not included in Appendix A.

The relative effectiveness and significance of specific controls for the managed services at WESCO Net and their effect on assessments of control risk at user organizations are dependent on their interaction with the controls and other factors present at individual user organizations. We have performed no procedures to evaluate the effectiveness of controls at individual user organizations.

The description of controls for the managed services at WESCO Net is as of June 30, 2010, and information about tests of the operating effectiveness of specified controls covers the period from January 1, 2010 to June 30, 2010. Any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the controls in existence. The potential effectiveness of specified controls for the managed services at WESCO Net is subject to inherent limitations and, accordingly, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that changes may alter the validity of such conclusions.

This report is intended solely for the use of management of WESCO Net, its customers, and the independent auditors of its customers.

A handwritten signature in black ink that reads "Crowe Horwath LLP". The signature is written in a cursive, flowing style.

Crowe Horwath LLP

South Bend, Indiana  
September 30, 2010

## DESCRIPTION OF CONTROLS PLACED IN OPERATION

*Provided by WESCO Net*

### OVERVIEW OF OPERATIONS

CU\*Answers, Inc., formerly West Michigan Computer CO-OP, Inc. (WESCO) and dba WESCO Net for managed network services is a data processing service organization chartered as both a Credit Union Service Organization (CUSO) and a cooperative. The organization is currently owned by 86 credit unions. Each credit union represents only one leadership vote, and has the right to be represented by its professional managing executive as a member of CU\*Answers' Board of Directors. There are seven seats on CU\*Answers' Board of Directors and members are elected to serve three-year terms. This style of direction creates a client-focused organization with an emphasis on services that are consultative, credit union industry focused, and dedicated to a "think tank" approach to data processing services and their application.

CU\*Answers has been providing core and peripheral data processing services to its client credit unions since 1970.

CU\*Answers, through its WESCO Net division, also provides a complete offering of network management services. WESCO Net is a full-service network technology solutions provider specializing in LAN/WAN design, implementation and management; network security; firewall management; cloud-based services and storage; IP telephony VOIP (voice-over-Internet protocol) solutions; electronic records management; managed hosting solutions (facilities management), compliance and security audits (HIPAA/GLBA/SOX); technology strategic planning services, remote support services, high availability solutions; web site engineering, server, storage, network, PC hardware sales and support services.

WESCO Net provides services to the education, retail, legal, medical, real estate, hospitality, and financial services industries as well as court systems and regional municipalities. WESCO Net has a nationwide network reach with 24x7 real-time monitoring and management of thousands of devices and hundreds of networks across the U.S.

WESCO Net also provides compliance expertise with policy development, implementation, and consulting services for highly regulated industries. It has expertise in implementation of proven high availability solutions for critical applications whether hosted at WESCO Net's state-of-the-art data center facilities or on-premise.

Data security is a top priority at WESCO Net, and permeates everything we do. Because security is such a complex issue, no single solution or "silver bullet" can be expected to provide adequate protection. As such, we view security much like an onion: it should have many layers each providing additional levels of protection.

The first layer in any organization are knowledgeable network administrators experienced in applying security best practices to network resources. Our IT staff continuously monitors CERT and other third party advisories for the latest security bulletins and alerts in addition to regular research and application of the latest security standards. Additionally, technical staff members are encouraged to seek appropriate external security training.

## DESCRIPTION OF CONTROLS PLACED IN OPERATION

*Provided by WESCO Net*

Additional security layers for facilities management devices include border and gateway devices secured to industry best-practices, dual redundant gateway firewalls, network and host based intrusion detection systems, layered network firewalls, hosts secured to industry best-practices and kept up to date with critical security fixes, daily log file reviews, centrally managed enterprise-wide anti-virus software updated hourly, centralized critical event log file aggregation systems, centralized device performance and response monitoring and alerting, and regular internal host configuration security audits.

To independently verify our security, WESCO Net contracts with independent third parties to perform periodic external and internal penetration tests. These assessments identify potential targets, probe those targets to determine their configuration and identify vulnerabilities, and finally attempt to exploit discovered vulnerabilities. WESCO Net management reviews the results of each assessment and implements necessary recommendations as suggested.

The final, and most important, security layer in any organization is a security-conscious and trained staff. All the firewalls in the world will not stop an uninformed, careless, or reckless employee from accidentally disclosing important information or succumbing to social engineering attacks. Because WESCO Net recognizes this threat, our on-staff security experts have crafted an aggressive security awareness campaign that includes comprehensive courses covering everything from security basics to advanced network defense principles and teaches these to both staff and clients alike. This campaign is an essential ingredient for creating and maintaining an attitude of "security is our way of doing business."

From network design to security consulting to a complete outsourcing of entire networks, WESCO Net has a solution for both credit unions and companies outside the credit union market. WESCO Net also provides an entire suite of products for web based applications and hosting services.

### **Managed Hosting**

#### *Infrastructure:*

WESCO Net maintains a highly available network infrastructure utilizing redundant Internet connections via fiber backbones, multiple ISPs to provide divergent routes to the Internet, redundant routers utilizing BGP 4 technology, redundant Checkpoint™ border gateway firewalls with Application Intelligence™ to provide Layer 7 security and integrated intrusion prevention, and optionally available redundant F5™ BIG-IP™ load balancing hardware for high availability applications, real-time failover, traffic load-balancing over multiple servers, and custom traffic directing rules to support any web-enabled application as well as an available SSL (Secure Sockets Layer) accelerator hardware to improve performance of secure web applications. WESCO Net's network has been engineered for virtualized technologies and supports VM Ware™, Microsoft's Hyper-V™, and Virtual Box™. WESCO Net's cloud computing infrastructure leverages highly scalable SAN and NAS technologies with select virtualization technologies to provide a flexible and secure managed storage and compute services environment.

## DESCRIPTION OF CONTROLS PLACED IN OPERATION

*Provided by WESCO Net*

### *Technical Security:*

Maintaining system integrity and security is a top priority at WESCO Net. Significant effort is made in establishing and maintaining a secure facilities infrastructure.

Therefore WESCO Net implements security in a layered approach which includes at least the following:

- Secure network architecture designed by security experts
- Systems segregated by task
- Controlled physical access to data centers and systems
- Controlled network access to all systems by enterprise-grade firewall and router systems
- Technical filters control all outgoing and incoming network traffic to help prevent unauthorized use
- Securing of the underlying operating system against known or possible attack by using the manufacturer's best practice recommendations
- Disabling or removing all unnecessary applications and services
- Security review of applications for known vulnerabilities and configuration errors
- Host-based intrusion detection: all access to the host system is logged and reviewed daily. As a method of verifying file integrity clients can opt to be sent daily emails that chronicle file level changes on the system to compare with work they did.
- Systems are patched monthly and kept up to date with the latest software updates
- Network-based intrusion detection alerts administrators to attacks
- Network-based intrusion prevention thwarts certain known attacks
- Anti-virus systems scan network, host, and PC traffic and content in real time for virus activity. Pattern files are updated hourly.
- A proactively trained and alert staff on the latest security vulnerabilities and responses.

An additional security layer for all managed hosting customers is a dedicated WESCO Net managed firewall with a customized rule-set for the environment. Redundant highly-available firewalls are also available.

### *Physical Security:*

WESCO Net employs multi-level building access controls including:

- All guests must sign-in, wear visitor badges and be escorted at all times
- Employees must use electronic security keys to enter main building, and various secure areas throughout the center
- Access point activities are centrally logged and monitored
- Video surveillance to DVR is used throughout the facilities to monitor activity

## DESCRIPTION OF CONTROLS PLACED IN OPERATION

*Provided by WESCO Net*

- Access to computer room is controlled through key code panels or electronic security keys
  - Operators staff the production datacenter 24x7 and monitor secondary access
  - Only authorized employees are permitted access
  - Employees who do not work in the datacenter are required to sign in and wear I.D. badges while in the facility

### *Training:*

People are the closest security layer to the data, and social engineering attacks have historically been the most effective way to compromise networks. Therefore both technical and non-technical staff is regularly trained on the latest security techniques and procedures and social engineering tactics and defenses.

### *Two-Stage Network Backups*

WESCO Net's backup solution uses an innovative two-stage architecture whereby backups are made to high speed network attached storage (NAS) devices, thereby shortening backup windows by up to 50% and then optionally archived to tape for offsite storage. Restores from NAS offer high-speed "point and click" data or system recovery.

Backups are automated and run from a centralized backup server.

1. Data is backed up across the local network to a secure NAS device. Data is maintained on disk for up to 10 days. Disk backups offer short backup windows and fast restores. Data on the wire can be encrypted if desired.
2. Data on the NAS is then archived to LTO tape weekdays for offsite storage. Standard data retention is 21 days (longer retention periods available upon request).

The WESCO Net Technical Services Division focuses on providing services to its client base. Network Solutions and Software Design members are added to the staff based on the combination of both their general technical skills and their understanding of the managed services industry. The Technical Division also includes accounting, marketing, and administration specialists that focus on their interest in the managed services industries and their unique disciplines to ensure that WESCO Net clients receive services that are in line with the best the market has to offer.

Identification of Control Objectives related to the descriptions provided within this section are listed in Appendix A.

User Control Considerations which complement the internal controls of WESCO Net are listed in Appendix B.

## DESCRIPTION OF CONTROLS PLACED IN OPERATION

*Provided by WESCO Net*

### GENERAL CONTROLS

General Controls are those policies, procedures, and safeguards which relate to all Information Systems (IS) activities. They include Organization and Administration, Physical Security, Managed Hosting Services, Complete Care Management, Firewall Management Service and e-Business Policies and Procedures.

General Controls seek to ensure the continued, consistent, and proper functioning of information systems by controlling and protecting the maintenance of application software and the performance of computer operations. Because General Controls affect all IS activities, their adequacy is considered basic to the effectiveness of specific application controls. Furthermore, any weaknesses in General Controls can often have pervasive effects. It is important to understand the General Controls in evaluating controls over specific applications.

#### *Organization and Administration*

CU\*Answers is organized into eight functional groups: Administration/Human Resources Marketing, Technical Resources (Programming, Internal Networks & Software Design), Client Service, Item Processing (CU\*CHECK), Finance (Business Development and Accounting), Product Team (Documentation, Quality Control, Compliance), and Operations. The WESCO Net team is comprised of four functional groups within the Technical Resources division of CU\*Answers: Web Services, Systems/External Networks, Internal Networks, System-I (iSeries). For reference purposes, *Appendix C: Organizational Chart* is included. Either an Officer, Vice President or Department Manager controls each group, with each Vice President or Manager reporting directly to the Senior Management Team.

CU\*Answers has been organized as a credit union owned CUSO since 1970. A seven-member Board of Directors meets regularly to review company status. Each June, a Leadership Conference is held which provides clients a comprehensive project status review and highlights planning direction for CU\*Answers in the coming year. The Annual Stockholder Meeting has been conducted for more than ten years, and is also held in June. Additionally, interactive client Focus Group sessions and general meetings are scheduled periodically covering current topics of interest including data security. These meetings help assist CU\*Answers' management in addressing the needs of the users.

Planning activities are ongoing and reviewed as a standard part of management meetings. Each department head provides input for CU\*Answers management team's discussion topics. Examples of meeting topics discussed include client service review, conversion planning information, systems and operations topics, programming enhancements and modifications, and upcoming software release timing and education.

All employees are provided with a variety of manuals that include procedures for the departments in which they work. An Employee Handbook is distributed to all new employees and all documentation is also provided to the employees via a CU\*Answers hosted intranet.

## DESCRIPTION OF CONTROLS PLACED IN OPERATION

*Provided by WESCO Net*

Further, the CEO of the company conducts several meetings during the year which include discussions concerning employee training, benefits, audit issues, goals and strategic plans, as well as other corporate issues.

CU\*Answers maintains an insurance package that includes IS equipment, media, extra expense, general liability, building and contents casualty coverage, workmen's compensation, umbrella liability coverage, employee dishonesty coverage, and errors and omissions coverage.

### *Physical Security*

The WESCO Net Kentwood Service Center is located on the main floor of a one-floor office building. The center is staffed 24-hours per day, seven days per week. The entrances are locked at all times. Visitors can only gain entrance into the building when authorized by WESCO Net personnel. All visitors must sign in at the receptionist desk, and wear a "visitor" badge at all times while in the building. The security alarm is set at a specified time each evening securing the perimeter of the facility. Key employees are issued electronic building keys that allow access to the building on a five or seven day system. A building security officer maintains a log of all keys and their numbers.

The WESCO Net Grand Rapids Service Center is located on the lower level of a three-floor office building. The center is staffed 10-hours per day, five days per week. The entrances are locked at all times. Visitors can only gain entrance into the building when authorized by WESCO Net personnel. All visitors must sign in at the receptionist desk, and wear a "visitor" badge at all times while in the building. The security alarm is set at a specified time each evening securing the interior and perimeter of the facility. Employees are issued electronic building keys that allow access to the building on a five or seven day system. A building security officer maintains a log of all keys and their numbers.

The CU\*Answers Muskegon Service Center is located on the fifth level of a seven story office building. The center is a "dark" site for hosting redundant and backup systems and is not regularly staffed. The entrance is locked at all times. Visitors can only gain entrance into the building when authorized and escorted by CU\*Answers personnel. The security alarm is set at all times unless occupied by CU\*Answers support staff. Authorized employees are issued electronic building keys that allow access to the building on a seven day system. A building security officer maintains a log of all keys and their numbers.

Access to the computer rooms may be gained only by authorized employees using electronic building keys on the computer room door. Smoking, eating and drinking are prohibited in the computer room. Any non-operations staff must sign in at the computer room reception area.

Both the Kentwood and the Grand Rapids computer rooms are protected by a FM-200 fire suppression system. Additionally, all the buildings are directly linked to a local monitoring company via an alarm system. Sensors positioned throughout the building, including storage areas, detect heat, smoke, motion and immediately notify the local monitoring company who in

**DESCRIPTION OF CONTROLS PLACED IN OPERATION**  
*Provided by WESCO Net*

turn notifies the fire department and building security. The buildings are monitored 24-hours per day, seven days per week.

The buildings are also protected against fire by hand held extinguishers. These extinguishers are inspected in February of each year and may be used on electrical devices, liquids, and other combustible materials.

Emergency battery powered lighting, activated when the power is cut off, is located throughout all facilities. Signs posted above certain doors mark emergency exits. An Uninterrupted Power Supply (UPS) has been installed in each facility to provide power for the systems for up to 40 minutes in the event of a power failure. Natural gas powered electric generators are in place in Kentwood and Grand Rapids to supply continuous power to all critical systems for an unlimited amount of time. There are specific test procedures for the UPS and generator systems that are detailed in the Disaster Recovery Manual.

***Managed Hosting Services (aka Facilities Management)***

Daily backups are performed for all Intel-based servers including facilities management clients. Backups are written to high speed disk drives using Network Attached Storage (NAS) devices and maintained for up to 10 days. Daily backups of the NAS devices are made to tape. Tapes are maintained offsite for 14 days then returned to the originating facility for reuse.

Network Security Domains

WESCO Net segregates client networks by security domain using routing application-aware stateful inspection firewalls. These security domains are used to control ingress/egress traffic and are constructed based on role. For example web servers will typically be grouped into a security domain and file and database servers into another.

Each security domain will consist of a subnet of network addresses as predetermined by network administrators and as tracked in the IP Address Allocation Schedule spreadsheet. The typical deployment of a managed hosting network is to place a security appliance on an existing network segment (such as a web security zone) behind the core firewalls. The security appliance then would have LAN and DMZ security domains, as appropriate, based on the required role(s). The dedicated client security appliance would then be used primarily to:

1. Provide controls for traffic leaving the hosted client security domain for the purpose of preventing unauthorized traffic to adjoining security domains behind the core firewall.
2. Provide a VPN end point for client networks that connect to the hosted network.
3. Provide controls for traffic taking place between LAN and DMZ security domains of the security appliance (i.e. between a web server and a database server.)
4. Provide an auditing point for traffic traversing security domains.

**DESCRIPTION OF CONTROLS PLACED IN OPERATION**  
*Provided by WESCO Net*

Management Tools

WESCO Net uses a variety of tools to manage its network. Clients generally do not have access to these tools though it is permissible to allow the network monitoring system to send availability email alerts to clients and to provide historical graphing information with the approval of the VP of Network Technology. WESCO Net has deployed Latitude, a web-based Management Portal for online client access to reports and help desk systems.

Daily Operational Procedures

The following procedures must be executed every week day on all client Intel systems. The purpose of these procedures is to maintain the safe, secure, and ongoing operating environment for all network assets under our management. Anomalies must be investigated and errors reported, escalated, and remediated on a daily basis. Errors allowed to continue may create an unstable environment and may cause failures.

1. Follow run sheets for each system
2. Respond to network monitoring system alerts as appropriate
3. Run backups following established procedures and review network backup system logs
4. Review Intrusion Detection System logs

Monthly Operational Procedures

Monthly run sheets have been developed to document the following:

1. Systems will be patched according to predetermined schedule, currently third Tuesday of every month from 1-8 AM
2. Patches will be downloaded automatically and installed manually by Administrator unless other arrangements are made
3. Administrators will verify patch installation by checking application and system logs for relevant entries and will occasionally run Microsoft Baseline Security Analyzer against the system for further verification.
4. All critical patches will be installed. Optional patches will be installed at the discretion of the administrator depending on the severity and applicability of the update.
5. Drivers must not be installed unless approved by the hardware vendor
6. Unsuccessful patches will be worked until successful unless determined non-critical by the administrator.

## DESCRIPTION OF CONTROLS PLACED IN OPERATION

*Provided by WESCO Net*

### Client Change Requests

It is not often that request for system or network changes are submitted by managed hosting clients, as most manage their own applications and will install/remove software at their own discretion. They are also administrators on their systems and can make configuration changes at will and handle their own password resets.

The majority of client requests will be for assistance troubleshooting a problem and prompt responses by WESCO Net administrators is expected. Client request are submitted via the Latitude Help Desk Portal and are tracked to completion.

### Unscheduled Maintenance

Unscheduled maintenance that would affect system availability or interfere with contractual obligations must be communicated to the client at least 24 hours in advance, though at least a week's notice is preferred. Care is taken not to perform maintenance on client systems during known critical production cycles.

### *Firewall Management Service*

WESCO Net Firewall management is an on-premise managed security service which provides 24x7x365 proactive monitoring and administration for firewall infrastructure. The service includes the following service and deliverables:

- Provides a comprehensive, integrated network security solution against advanced threats by employing; High-bandwidth stateful packet inspection.
- Deep Packet Inspection Technology
- Intrusion Prevention/Detection
- Gateway Anti-Virus
- Gateway Anti-Spyware
- Policy based application filtering
- Firewall policy design and Technical Assistance
- 24x7x365 Monitoring with Secure Offsite Log Storage
- 10x5 Support Standards, with 24x7 support optional
- VPN/Remote User Management
- Complete Hardware Warranty and Replacement
- Firmware Upgrades
- Automatic Configuration Control and Backup
- Comprehensive Scheduled and On-Demand Reporting
- Real Time Alerting
- Strategic Network Planning

## DESCRIPTION OF CONTROLS PLACED IN OPERATION

*Provided by WESCO Net*

All managed equipment is placed on-premise at the client site and subject to client's physical and environmental security controls. WESCO Net recommends following industry standard best practices to address physical and environment security.

### Infrastructure

WESCO Net's firewall management monitoring and reporting system resides on a secured network segment within the CU\*Answers corporate network at the Kentwood datacenter. The firewall management system consists of a front-end web console server and a backend database server. WESCO Net is using the firewall Global Management System software to monitor and manage client firewalls, collect network traffic data, track subscription licensing and provide reporting. Client firewalls transfer Syslog data in real-time via IPSEC or HTTPS encrypted tunnel. The tunnel connections are terminated at redundant Enterprise NSA-class firewalls.

WESCO Net maintains all Syslog data collected from client firewall systems for a minimum of 30 days.

### Operational Procedures

The following procedures are executed according to published schedule for all managed units. The purpose of these procedures is to maintain the safe, secure, and ongoing operating environment for all network assets under WESCO Net management. Anomalies must be investigated and errors reported, escalated, and remediated on a daily basis. Errors allowed to continue may create an unstable environment and may cause failures. WESCO Net's monitoring and management infrastructure is configured to open trouble tickets and/or issue alerts when certain thresholds are met on managed systems.

1. Review report distribution, make client contact for any down units
2. Process all client change requests
3. Installation/upgrade of any firmware or software available
4. Resolution of any trouble tickets generated from server monitoring system
5. Review firewall management system logs
6. Conduct a quarterly audit of firewall settings, to ensure licenses and services are synchronized and available and review firmware version. Results are recorded and available for client review.
7. Weekly run sheets have been developed to document the following:
  - a. Systems will be patched according to a predetermined schedule, daily, as updates are available at 10pm
  - b. Patches will be downloaded automatically and installed manually by Administrator unless other arrangements are made
  - c. Administrators will verify patch installation by checking application and system logs for relevant entries and will occasionally run Microsoft Baseline Security Analyzer against the system for further verification.

## DESCRIPTION OF CONTROLS PLACED IN OPERATION

*Provided by WESCO Net*

- d. All critical patches will be installed. Optional patches will be installed at the discretion of the administrator depending on the severity and applicability of the update.
- e. Drivers must not be installed unless approved by the hardware vendor
- f. Unsuccessful patches will be worked until successful unless determined non-critical by the administrator.

### *Complete Care Management*

WESCO Net's Complete Care Management is an on-premise managed security service. The service includes the following service and deliverables:

- 24x7x365 monitoring and alerting for all network connected devices and critical services
- Server and workstation patching (24-hour response for critical and security related patches)
- Weekly Server Security Baseline testing
- Real time Backup Log monitoring and remediation
- Real time Anti-Virus monitoring including virus pattern version and unprotected machines
- Unlimited Group and User Management
- Quarterly Backup File Restore and Virtualization Testing w/Report
- Quarterly 3<sup>rd</sup> Party Vulnerability Scanning for Public Facing Network Devices
- 3<sup>rd</sup> Party Vulnerability Scanning for Internal Network Devices
- Weekly Systems Review
- Weekly Full Finding Report

All managed equipment is placed on-premise at the client site and subject to client's physical and environmental security controls. WESCO Net recommends following industry standard best practices to address physical and environment security.

### Infrastructure

WESCO Net's Complete Care monitoring and reporting system resides on a secured network segment within the CU\*Answers corporate network at the Kentwood datacenter. The Complete Care management system consists of a front-end web console server and a backend database server. WESCO Net utilizes Level Platforms Managed Workplace platform. Client devices transfer all Syslog, WMI and SNMP data in real-time via HTTPS encrypted tunnel. The tunnel connections are terminated at the front-end web server. The management platform resides behind a high availability pair of Enterprise NSA firewalls.

WESCO Net maintains all data collected from client systems for a minimum of 90 days.

## DESCRIPTION OF CONTROLS PLACED IN OPERATION

*Provided by WESCO Net*

### Operational Procedures

The following procedures are executed according to published schedule for all managed units. The purpose of these procedures is to maintain the safe, secure, and ongoing operating environment for all network assets under our management. Anomalies must be investigated and errors reported, escalated, and remediated on a daily basis. Errors allowed to continue may create an unstable environment negatively affecting the overall security posture of the client site. WESCO Net's monitoring and management infrastructure is configured to open trouble tickets and/or issue alerts when certain thresholds are met or exceeded on managed systems.

1. Review trouble tickets and alerts
2. Process all client change requests
3. Review critical and security related patch availability
4. Daily review of system status, including event logs, backup systems, security baseline report and anti-virus systems
5. Weekly report review and delivery
6. Quarterly backup restore tests

### Client Change Requests

Client change requests are regularly received from Complete Care and firewall management clients. WESCO Net uses a secure, web based client management portal to receive these requests. Users with the ability to submit requests for information or configuration changes must have prior authorization from their institution. WESCO Net technical staff has the ability to open support tickets based on email from authorized clients on behalf of that client. WESCO Net technical support staff is required to ensure client requests have been logged in Latitude prior to completing the request. Clients have the ability to track the status of their tickets through the portal at any time. All client requests are archived to ensure a clear audit trail. Clients have the ability to review their past request history and can request a custom report on this activity at any time.

The majority of client requests are for assistance troubleshooting a problem or for configuration changes and prompt responses by WESCO Net administrators is expected.

### SGMS Infrastructure Backups

The Complete Care and firewall management servers are part of WESCO Net's high availability backup solution, which uses a continuous data protection strategy, whereby encrypted system snapshots are made to local, high speed network attached storage (NAS) device in 15 minute increments. Every 24 hours, the incremental backups are compressed and transferred to an offsite via high-speed encrypted connection.

## DESCRIPTION OF CONTROLS PLACED IN OPERATION

*Provided by WESCO Net*

The system offers restore capabilities for multiple file versions, in 15 minutes up to the first 2 days and daily versioning the two most recent weeks. The backup system is monitored 24x7 and a ticket is automatically generated for missed backup or any issue with the backup system

The local and remote NAS devices also offer backup virtualization capabilities, facilitating a business continuity strategy for critical hardware or environmental failures at the primary site. Data backup integrity, recovery and virtualization are tested on the backup appliances on a quarterly basis.

### System Maintenance

All planned maintenance, including hardware, operating system or application upgrades is preceded by an announcement at least 8 hours prior to start. Any system maintenance that will result in downtime is scheduled at least 24 hours and preceded by an announcement. Care is taken not to perform maintenance on client systems during known critical production cycles.

### *e-Business Policies and Procedures*

Data security is a top priority at WESCO Net, and permeates everything we do. Because security is such a complex issue, no single solution or “silver bullet” can be expected to provide adequate protection. As such, we view security much like an onion: it should have many layers each providing additional levels of protection.

The first layer in any organization is a knowledgeable network administrators experienced in applying security best practices to network resources. Our IT staff continuously monitors CERT and other third party advisories for the latest security bulletins and alerts in addition to regular research and application of the latest security standards. Additionally, technical staff members are encouraged to seek appropriate external security training.

Additional security layers for System-i, Intel-based, and managed hosting devices include border and gateway devices secured to industry best-practices, dual redundant gateway firewalls, network and host based intrusion detection systems, layered network firewalls in some segments, hosts secured to industry best-practices and kept up to date with critical security fixes, regular log file reviews, centrally managed enterprise-wide anti-virus software updated hourly, centralized critical event log file aggregation systems, centralized device performance and response monitoring and alerting, and regular internal host configuration security audits.

To independently verify security, WESCO Net contracts with an independent firm to perform periodic external and internal penetration tests. These assessments identify potential targets on Internet accessible devices, probe those targets to determine their configuration and identify vulnerabilities, and finally attempt to exploit discovered vulnerabilities. WESCO Net management reviews the results of each assessment and implements necessary recommendations as suggested.

## DESCRIPTION OF CONTROLS PLACED IN OPERATION

*Provided by WESCO Net*

The final, and most important, security layer in any organization is a security-conscious and trained staff. All the firewalls in the world will not stop an uninformed, careless, or reckless employee from accidentally disclosing important information or succumbing to social engineering attacks. Because WESCO Net recognizes this threat, on-staff security experts have crafted an aggressive security awareness campaign that includes comprehensive courses covering everything from security basics to advanced network defense principles and teaches these to both staff and clients alike. This campaign is an essential ingredient for creating and maintaining an attitude of “security is our way of doing business.”

**APPENDIX A  
ORGANIZATION AND ADMINISTRATION**

**CONTROL OBJECTIVE** -- WESCO Net and user functions are segregated.

<b>Controls Tested</b>	<b>Tests Performed</b>	<b>Sample/Population of Test</b>	<b>Test Results</b>
<p>WESCO Net is physically separate from and operates independently of the user institutions for which it provides Co-location services.</p> <p>User organizations have contracts with WESCO Net that outline the responsibilities of both WESCO Net and the user organization.</p> <p>User personnel are only allowed in the computer room when accompanied by WESCO Net network personnel.</p>	<ol style="list-style-type: none"> <li>1. Reviewed policies of the organization and contractual obligations that exist between WESCO Net and user organizations.</li> <li>2. Reviewed contractual obligations and verified that contract exist between WESCO Net and user organizations.</li> <li>3. Discussed with management and observed access restrictions to the computer room</li> </ol>	<p>Inspected documents and reports indicating performance of the control and made inquiries of appropriate company personnel.</p> <p>Reperformed the application of the control by selecting a sample of user organizations and verifying that a current signed contract was on file.</p> <p>Inspected documents and reports indicating performance of the control and made inquiries of appropriate company personnel.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>

**APPENDIX A  
ORGANIZATION AND ADMINISTRATION**

**CONTROL OBJECTIVE --** Administrative policies and procedure are documented.

Controls Tested	Tests Performed	Sample/Population of Test	Test Results
<p>An organizational chart exists to define the reporting structure of the organization and the lines of segregation between functional areas.</p> <p>Job descriptions have been prepared for all personnel.</p> <p>WESCO Net has an employee handbook that describes the company's policies for hiring, termination, salary administration, performance reviews, vacation, employee benefits, building and system security, and discrimination and harassment.</p> <p>An acknowledgement form is in place that requires employees to sign stating they have read and understand the company's administrative policies as stated in the Employee Handbook.</p> <p>The service organization maintains insurance coverage for the building and contents, IS equipment, media reconstruction, extra expense, fidelity coverage, errors and omissions, and umbrella liability coverage.</p>	<ol style="list-style-type: none"> <li>1. Reviewed the organization chart for completion, accuracy and appropriateness to the situation.</li> <li>2. Reviewed employee job descriptions.</li> <li>3. Ascertained that an employee handbook existed and reviewed the manual for inclusion of key policies.</li> <li>4. Verified that a signed acknowledgement form is on file for the employees.</li> <li>5. Obtained copies of IS insurance policies and noted that effective dates and related coverage's were current.</li> </ol>	<p>Inspected documents and reports indicating performance of the control and made inquiries with appropriate personnel.</p> <p>Inspected documents and reports indicating performance of the control.</p> <p>Inspected documents indicating performance of the control and made inquiries of appropriate company personnel.</p> <p>Reperformed the application of the control by selecting a sample of employees and ensuring that a signed acknowledgement form is retained in the employee's file.</p> <p>Made inquiries of appropriate company personnel and inspected documents and reports indicating performance of the control.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>

**APPENDIX A  
ORGANIZATION AND ADMINISTRATION**

**CONTROL OBJECTIVE** -- Administrative policies and procedure are documented.

<b>Controls Tested</b>	<b>Tests Performed</b>	<b>Sample/Population of Test</b>	<b>Test Results</b>
	6. Confirmed coverage's with all appropriate third party insurance companies.	Obtained the insurance confirmation from third party carrier and verified that coverage noted in the confirmation agrees to the policies reviewed.	No relevant exceptions noted.

**APPENDIX A  
PHYSICAL SECURITY**

**CONTROL OBJECTIVE** -- Safeguards and/or procedures are used to protect the service organization against intrusions, fire and other hazards.

Controls Tested	Tests Performed	Sample/Population of Test	Test Results
<p>All doors to the service organizations main and backup facility are locked and controlled by a security system.</p> <p>Authorized personnel have been issued electronic building keys and have been given the code to deactivate the perimeter alarm system at the facilities.</p> <p>The computer rooms are locked at all times and visitors must be admitted to the area by operations personnel.</p> <p>Heat, smoke, FM200 automated suppression system and intrusion detectors are connected to a monitored alarm system to the computer room facilities. Further, hand held fire extinguishers are located throughout the facilities.</p>	<ol style="list-style-type: none"> <li>1. Interviewed management, reviewed policies relating to physical security procedures and devices, and schedules of operation, and observed security systems and procedures.</li> <li>2. Discussed with management that only appropriate personnel have access to the buildings.</li> <li>3. Observed physical security procedures throughout the audit and verified the compliance with service organization policies and procedures.</li> <li>4. Toured the entire CU*Answers facilities and computer rooms and noted the presence and location of portable fire extinguishers (recent inspection), fire detection sensors and alarms, FM200 suppression, electrical power shut-off switch, analog phone line in the computer room, emergency lighting, and exit signs.</li> </ol>	<p>Made inquiries of appropriate company personnel and observed application of specific controls.</p> <p>Made inquiries of appropriate company personnel.</p> <p>Made inquiries of appropriate company personnel and observed application of specific controls.</p> <p>Observed application of specific controls.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>

**APPENDIX A  
PHYSICAL SECURITY**

**CONTROL OBJECTIVE** -- Safeguards and/or procedures are used to protect the service organization against intrusions, fire and other hazards.

Controls Tested	Tests Performed	Sample/Population of Test	Test Results
A written action plan relating to emergency situations is distributed to employees.	5. Reviewed the emergency action plan for adequacy and content. Determined that the plan included actions to be taken (e.g., equipment restart and recovery procedures), individuals to phone, and materials to be removed from the computer room.	Inspected documents and reports indicating performance of the control and made inquiries of appropriate company personnel.	No relevant exceptions noted.
An Uninterruptible Power Supply (UPS) system with power conditioners is installed to protect both computer room facilities from short or long-term power failures.	6. Toured the service organization and computer room and noted the presence and location of an UPS system.	Observed application of specific controls.	No relevant exceptions noted.
A natural gas generator is installed at each facility to protect the buildings from power failures.	7. Inspected the results of the last UPS inspections for each facility to ensure both UPS systems are being maintenance.	Inspected documents and reports indicating performance of the control and made inquiries of appropriate company personnel.	No relevant exceptions noted.
	8. Toured the service organization and noted the presence of a natural gas generator and discussed with management the weekly testing of the generator.	Observed application of specific controls and made inquiries of appropriate company personnel.	No relevant exceptions noted.
	9. Inspected the results of the last generator inspections for each facility to ensure both generators are being maintenance.	Inspected documents and reports indicating performance of the control and made inquiries of appropriate company personnel.	No relevant exceptions noted.

**APPENDIX A  
MANAGED HOST SERVICES (aka FACILITIES MANAGEMENT)**

**CONTROL OBJECTIVE** -- Controls are in place for managing server backups and ensuring appropriate network segmentation is in place.

Controls Tested	Tests Performed	Sample/Population of Test	Test Results
<p>All critical systems and applications on Intel (server) network are backed up daily. A file retention schedule and a schedule for premise rotation of system and/or application have been established.</p> <p>Backup logs are monitored and reviewed on a daily basis. File restore test of backup data are performed on a quarterly basis.</p> <p>WESCO Net segregates client networks by security domain using routing application-aware stateful inspection firewalls. These security domains are used to control ingress/egress traffic and are constructed based on role.</p>	<ol style="list-style-type: none"> <li>1. Verified the off-site presence and timeliness of the network server backups.</li> <li>2. Observed the physical protection of the off-site backup location.</li> <li>3. Verified procedures for reviewing the systems backup logs.</li> <li>4. Discussed with management procedures for performing quarterly file restore test of backup data.</li> <li>5. Ascertained that client networks are segregated by reviewing the firewall settings and network diagrams.</li> </ol>	<p>Reperformed the application of the control by inspecting backup tapes at the off-site facility.</p> <p>Observed application of specific controls.</p> <p>Reperformed the application of the control by selecting a sample of days and verified review of system backup logs by appropriate company personnel.</p> <p>Inspected documents and reports indicating performance of the control and made inquiries of appropriate company personnel.</p> <p>Inspected documents and reports indicating performance of the control and made inquiries of appropriate company personnel.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>

**APPENDIX A**  
**MANAGED HOST SERVICES (aka FACILITIES MANAGEMENT)**

**CONTROL OBJECTIVE** -- Controls are in place for managing server backups and ensuring appropriate network segmentation is in place.

Controls Tested	Tests Performed	Sample/Population of Test	Test Results
<p>Each security domain will consist of a subnet of network addresses as predetermined by network administrators and as tracked in the IP Address Allocation Schedule spreadsheet.</p>	<p>6. Discussed with network administrators procedures for configuring security domain and inspected the IP Address Allocation Schedule spreadsheet used for tracking.</p>	<p>Inspected documents and reports indicating performance of the control and made inquiries of appropriate company personnel.</p>	<p>No relevant exceptions noted.</p>

**APPENDIX A  
FIREWALL MANAGEMENT SERVICE**

**CONTROL OBJECTIVE** -- Intrusion prevention, anti-virus and anti-spyware monitoring have been implemented on the firewall and/or gateway equipment. Content Filtering has been configured and implemented.

Controls Tested	Tests Performed	Sample/Population of Test	Test Results
<p>Application or hardware systems have been configured to monitor the following items:</p> <ul style="list-style-type: none"> <li>• Intrusion Prevention Monitoring</li> <li>• Gateway Anti-Virus Monitoring</li> <li>• Gateway Anti-Spyware Monitoring</li> </ul> <p>Firewall and additional security devices (e.g., routers, and authentication servers) have been configured to appropriately restrict access from the Internet, user institutions, and business partners.</p> <p>Firewall policy changes, technical assistance and VPN management are authorized and tracked within the Latitude issue tracking system.</p>	<ol style="list-style-type: none"> <li>1. Obtained and inspected firewall configuration monitoring settings and discussed settings with network administrator.</li> <li>2. Obtained and inspected firewall configuration settings and discussed settings with network administrator.</li> <li>3. Interviewed network management regarding procedures for documenting firewall policy changes in the Latitude issue tracking system.</li> <li>4. Verified that changes made to the firewall policy are documented within the Latitude issue tracking system.</li> </ol>	<p>Inspected documents and reports indicating performance of the control and made inquiries of appropriate company personnel.</p> <p>Inspected documents and reports indicating performance of the control and made inquiries of appropriate company personnel.</p> <p>Inspected documents and reports indicating performance of the control and made inquiries of appropriate company personnel.</p> <p>Reperformed the application of the control by inspecting a sample of firewall policy changes and verifying they were appropriately entered into the Latitude issue tracking system.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>

**APPENDIX A  
FIREWALL MANAGEMENT SERVICE**

**CONTROL OBJECTIVE** -- Intrusion prevention, anti-virus and anti-spyware monitoring have been implemented on the firewall and/or gateway equipment. Content Filtering has been configured and implemented.

<b>Controls Tested</b>	<b>Tests Performed</b>	<b>Sample/Population of Test</b>	<b>Test Results</b>
Hardware warranty's are in place for firewall systems.	5. Obtained and reviewed maintenance agreement for firewall devices.	Inspected documents and reports indicating performance of the control and made inquiries of appropriate company personnel.	No relevant exceptions noted.
WESCO Net implemented industry standard firewall systems to monitor and control traffic between all network segments including the production networks, managed hosting networks, and the Internet.	6. Ascertained that client networks are segregated by reviewing the firewall settings and network diagrams.	Inspected documents and reports indicating performance of the control and made inquiries of appropriate company personnel.	No relevant exceptions noted.
The firewall is set up to log suspicious and unauthorized access attempts. Network Administrators review the firewall logs on a daily basis.	7. Verified procedures for reviewing the firewall logs.	Reperformed the application of the control by selecting a sample of days and verified review of firewall logs by appropriate company personnel.	No relevant exceptions noted.
Firewalls firmware is updated and backed up on a periodic basis.	8. Interviewed network management regarding procedures for backing up and updating firewall firmware.	Inspected documents and reports indicating performance of the control and made inquiries of appropriate company personnel.	No relevant exceptions noted.

**APPENDIX A  
COMPLETE CARE MANAGEMENT**

**CONTROL OBJECTIVE** -- Critical data servers (file servers, email, database, etc) are configured and kept up to date as new service packs and critical manufacturer fixes are released. Anti-virus systems are operational.

Controls Tested	Tests Performed	Sample/Population of Test	Test Results
Servers are patched with latest critical and security updates within 24 hours of the patch being released.	1. Discussed with network administrators procedures for applying network server and device patches.	Made inquiries of appropriate company personnel.	No relevant exceptions noted.
Server hardware and critical services are automatically inspected every 5 minutes. Security tests are executed against the servers on a weekly basis.	2. Interviewed network administrators regarding procedures for inspecting server hardware and critical services.	Made inquiries of appropriate company personnel and inspected documents and reports indicating performance of the control.	No relevant exceptions noted.
System and device logs are configured to record specified system events and the logs are retained both on the system and on a central log file aggregation device.	3. Discussed with network administrators procedures for configuring system logs and inspected the device configuration logs.	Inspected documents and reports indicating performance of the control and made inquiries of appropriate company personnel.	No relevant exceptions noted.
WESCO Net monitors and audits network systems, including managed hosting networks, for configuration changes, current anti-virus pattern files, resource utilization, significant system events, invalid sign-on attempts and software patch levels.	4. Verified procedures for reviewing the network systems performance and security logs.	Reperformed the application of the control by selecting a sample of days and verified review of system logs by appropriate company personnel.	No relevant exceptions noted.
Anti-virus configurations are reviewed and updated weekly; a scan of all network devices is performed weekly to determine virus pattern, scan engine version and locate any unprotected workstations.	5. Discussed with network administrators procedures for configuring anti-virus and inspected the anti-virus configuration settings.	Inspected documents and reports indicating performance of the control and made inquiries of appropriate company personnel.	No relevant exceptions noted.

**APPENDIX A  
COMPLETE CARE MANAGEMENT**

**CONTROL OBJECTIVE** -- Critical data servers (file servers, email, database, etc) are configured and kept up to date as new service packs and critical manufacturer fixes are released. Anti-virus systems are operational.

Controls Tested	Tests Performed	Sample/Population of Test	Test Results
<p>Various monitoring reports are supplied to the client on a periodic basis. Reports are automatically generated and delivered by our firewall management reporting servers, on a daily, weekly and/or monthly basis via email.</p>	<p>6. Reports are created and delivered on a periodic basis that contain the following items:</p> <ul style="list-style-type: none"> <li>• Patch Management</li> <li>• Server Backup Results</li> <li>• Vulnerability Scans</li> <li>• Server Activity Results</li> </ul>	<p>Reperformed the application of the control by selecting a sample of 28 weeks and clients and verified that the appropriate reports were generated.</p>	<p>During our review of the managed services weekly reports provided to clients, we found that one client was not provided all the required reports for the week of February 11, 2010.</p> <p><u>Management Response:</u></p> <p>This was a one-time error and the employee was appropriately reprimanded.</p> <p>Management has implemented a policy of having a second person review the managed service reports to ensure all reports are sent to clients.</p>

**APPENDIX A  
COMPLETE CARE MANAGEMENT**

**CONTROL OBJECTIVE** -- System security management is performed per the request of the client.

Controls Tested	Tests Performed	Sample/Population of Test	Test Results
<p>Client change requests are regularly received from Complete Care and firewall management clients. WESCO Net uses a secure, web based client management portal, Latitude, to receive these requests.</p> <p>Users with the ability to submit requests for information or configuration changes must have prior authorization from their institution. WESCO Net technical staff has the ability to open support tickets based on email from authorized clients on behalf of that client.</p> <p>Latitude issue report is created on a weekly basis documenting any issues reported and distributed to the client.</p> <p>All client requests are archived to ensure a clear audit trail. Clients have the ability to review their past request history and can request a custom report on this activity at any time.</p>	<ol style="list-style-type: none"> <li>1. Interviewed network management regarding procedures for documenting client change request in the Latitude issue tracking system.</li> <li>2. Interviewed network management regarding procedures for documenting client change request in the Latitude issue tracking system.</li> <li>3. Verified that issue report is generated and provided to the client on a weekly basis.</li> <li>4. Interviewed network management regarding procedures for archiving client Latitude issues.</li> </ol>	<p>Inspected documents and reports indicating performance of the control and made inquiries of appropriate company personnel.</p> <p>Inspected documents and reports indicating performance of the control and made inquiries of appropriate company personnel.</p> <p>Reperformed the application of the control by selecting a sample of weeks and clients and verified that the Latitude issue report was generated.</p> <p>Observed application of specific controls and made inquiries of appropriate company personnel.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>

**APPENDIX A**  
**e-BUSINESS POLICIES AND PROCEDURES**

**CONTROL OBJECTIVE** - Policies and procedures to address e-Business risk are documented, communicated, and provided to the staff.

Controls Tested	Tests Performed	Sample/Population of Test	Test Results
<p>Policies and procedures for e-Business activities are documented, reviewed by management, and provided to CU*Answers staff.</p> <p>CU*Answers implemented an industry standard firewall systems to monitor and control traffic between all network segments including the production networks, managed hosting networks, and the Internet.</p> <p>The firewall is set up to log suspicious and unauthorized access attempts. Network Administrators review the firewall logs on a daily basis.</p> <p>A firewall and additional security devices (e.g., routers, and authentication servers) have been configured to appropriately restrict access from the Internet, user institutions, and business partners.</p>	<ol style="list-style-type: none"> <li>1. Reviewed e-Business Policies and Procedure documents.</li> <li>2. Discussed with management the configuration of the firewall and the monitoring controls.</li> <li>3. Discussed with management policies and procedures for reviewing the firewall logs.</li> <li>4. Verified procedures for reviewing the firewall logs.</li> <li>5. Discussed security configurations with management and reviewed the annual Penetration Study Report.</li> </ol>	<p>Made inquiries of appropriate company personnel and inspected documents and reports indicating the performance of the controls.</p> <p>Made inquiries of appropriate company personnel and inspected documents and reports indicating the performance of the controls.</p> <p>Made inquiries of appropriate company personnel.</p> <p>Reperformed the application of the control by selecting a sample of days and verified review of firewall logs by appropriate company personnel.</p> <p>Made inquiries of appropriate company personnel and inspected documents and reports indicating the performance of the controls.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>

**APPENDIX A**  
**e-BUSINESS POLICIES AND PROCEDURES**

**CONTROL OBJECTIVE** - Policies and procedures to address e-Business risk are documented, communicated, and provided to the staff.

Controls Tested	Tests Performed	Sample/Population of Test	Test Results
<p>System and device logs are configured to record specified system events and the logs are retained both on the system and on a central log file aggregation device.</p> <p>CU*Answers security administrators review the network server systems and devices on a daily basis to detect inappropriate or unauthorized activity on the system.</p> <p>CU*Answers follows a change control procedure for firewall rule base changes and all policy changes are approved by management.</p>	<p>6. Interviewed management to determine policies and procedures regarding configuration of system logs.</p> <p>7. Interviewed management to determine policies and procedures regarding review of the system logs.</p> <p>8. Verified procedures for reviewing the network server system logs.</p> <p>9. Interviewed management and reviewed firewall policy change logs to determine policies and procedures regarding change control procedures for firewall rule base changes.</p>	<p>Made inquiries of appropriate company personnel and inspected documents and reports indicating the configuration of the system logs.</p> <p>Made inquiries of appropriate company personnel and inspected documents and reports indicating the performance of the controls.</p> <p>Reperformed the application of the control by selecting a sample of days and verified review of network server system logs by appropriate company personnel.</p> <p>Made inquiries of appropriate company personnel and inspected documents and reports indicating the configuration of the firewall.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>

## APPENDIX B - USER CONTROL CONSIDERATIONS

This section outlines specific User Control Considerations that may be appropriate at each user financial institution, along with the objective of the control. These considerations should not be regarded as a comprehensive list of all internal accounting controls that should be employed by users, or as representing procedures that are necessary in all circumstances.

1. WESCO Net customers are responsible for authorizing employees that are allowed physical access to the WESCO Net facility and responsible for communicating this list to WESCO Net.
2. WESCO Net customers are responsible for reporting to WESCO Net any changes in key contacts for communication purposes or terminations of employees who have been granted access to the facility.
3. WESCO Net customers are responsible for accompanying the "guests" that they bring into the WESCO Net datacenter facility. These guests are also required to sign the visitors log and receive a badge to identify themselves.
4. WESCO Net customers are responsible for establishing communications to the datacenter facility systems and for ensuring that redundant lines for backup communications exist.
5. WESCO Net customers should have a business continuity plan in place to ensure that their systems can be restored in the event of an unplanned disruption.
6. WESCO Net customers are responsible for reviewing activity reports and security findings reports that are provided by WESCO Net.
7. If WESCO Net is not authorized to perform backups, controls should be established for the creation of backup tapes to ensure that important business data would be available to recover after a disaster.
8. Facility management and Managed Services customers are responsible for ensuring that their network infrastructure deployed at WESCO Net provides an appropriate level of resiliency and redundancy.
9. Managed Services customers are responsible for designing their applications and systems to ensure they can be adequately supported given the Service Delivery Intervals outlined in the Description of Controls section of this document.
10. Managed Services customers are responsible for securing ongoing maintenance and support contracts for all non-WESCO Net-owned software and hardware.

## APPENDIX C - ORGANIZATIONAL CHART

